UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/385,591	08/29/1999	GARY L. GRAUNKE	42390.P7573	9395

7590 10/06/2003

ALOYSIUS T C AUYEUNG
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
7TH FLOOR
12400 WILSHIRE BOULEVARD
LOS ANGELES, CA 90025

EXAMINER	
KIM, JUNG W	
ART UNIT	**PAPER NUMBER**
2132	9

DATE MAILED: 10/06/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/385,591	GRAUNKE ET AL.	
	Examiner	Art Unit	
	Jung W Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-27 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-27 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 29 August 1999 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2-8 .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 110 and Mi-1. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

2. New corrected drawings are required in this application because the drawings are informal and are not in compliance with 37 CFR 1.84. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The formal drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Specification

3. The disclosure is objected to because of the following informalities: on page 11, line 5, the Specification refers to a Figure 5; no Figure 5 was submitted with the application. Appropriate correction is required.

4. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Claim Objections

5. Claims 23-25 are objected to because of the following informalities: dependent claims 24 and 25 state "...wherein the first plurality of transformation units comprise...", however, based on the parent claim and the disclosure of the invention in the specification, the claims should read "...wherein the second plurality of transformation units comprise..."; claims 23-25 discloses that the second plurality of transformation units are coupled to a first, second, and third register; however, the parent claim discloses that the second plurality of transformation units are coupled to a fourth, fifth, and sixth register. Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 2, 4-12, 14-19, and 21-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Feistel U.S. Patent No. 3,798,360 (hereinafter Feistel) in view of Coulthart et al. U.S. Patent No. 4,641,102 (hereinafter Coulthart). The invention disclosed by the claims are lacking in clearly identifying the invention as disclosed in the

specification. A substantial body of the claims read into well-known block ciphers, which utilize linear and non-linear transformations including classical Feistel ciphers and the Madryga cipher, as well as several RNGs.

8. As per claim 19, the apparatus disclosed in this claim is vaguely defined and reads into a step code cipher disclosed by Feistel. Feistel teaches the cipher as comprising:

a) a data section having a first, a second, and a third register to be collectively initialized with a random number, and a first plurality of transformation units coupled to the first, second and third registers to successively and dependently, on a first key section, transform the random number (see Feistel, col. 2, line 60-col. 4, line 26; Figure 1). Although Feistel discloses a first, a second and a third block as part of a feed register, he further elaborates in the disclosure that the segmentation of the data blocks are a matter of design choice (see Feistel, col. 4, lines 65-68); since these 3 blocks operatively function as 3 separate registers, they are interpreted as a first, a second, and a third register. Furthermore, Feistel discloses data first being loaded into feed register(s) then into transmit register(s) after data transformation (see Feistel, Figure 1), however, the cipher operation as disclosed by Feistel does not preclude the feed register(s) and the transmit register(s) as being the same. Since circuit reuse is a fundamental design goal, it would be obvious to use only a single set of registers to both store the data and the ensuing ciphertext.

b) a second key section coupled to the first key section to selectively modify a first cipher key (see Feistel, Figure 1, Reference Nos. 26, 44, 43, 42, 24, 22) and

c) a mapping section coupled to the first key section and the data section to generate a pseudo random bit sequence (see Feistel, Figure 1, steps 2 and 5, Reference No. 22; Figure 3A, 'Mangler').

Feistel does not cover a key section having a combination similar to the combination as defined in the data section above. However, key generators having three or more registers as well as transformation units coupled to these registers are conventionally found. Coulthart discloses such an example where a first key section has a fourth, a fifth, and a sixth register to be collectively initialized with a first cipher key, and a second plurality of transformation units coupled to the fourth, fifth, and sixth registers to successively transform a selectively modified version of the first cipher key (see Coulthart, Figure 1). In the invention disclosed by Coulthart, the fourth, fifth, and sixth registers are labeled as SR5, SR4, and SR3 respectively in Figure 1. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the key generator as disclosed by Coulthart with the ciphering system as defined by Feistel. The motivation for such a combination would allow for a simple RNG design given by Coulthart to be used as the random number generator in the invention for key generation as disclosed by Feistel.

The aforementioned covers claim 19.

9. As per claim 21, Feistel discloses a cipher system as outlined above in the claim 19 rejection under 35 U.S.C. 103(a). In addition, the second plurality of transformation units comprise a linear transformation unit coupling the fifth register to the fourth register to store a linearly transformed version of the content of the fifth register into the fourth register during a round of operation (see Coulthart, Figure 1, Reference Nos. SR4, E05, SR5).

10. As per claim 22, Feistel discloses a cipher system as outlined above in the claim 19 rejection under 35 U.S.C. 103(a). In addition, the second plurality of transformation units comprise a linear transformation unit coupling the sixth register to the fifth register to store a linearly transformed version of the content of the sixth register into the fifth register during a round of operation (see Coulthart, Figure 1, Reference Nos. SR3, E04, SR4).

11. As per claim 23, Feistel discloses a cipher system as outlined above in the claim 19 rejection under 35 U.S.C. 103(a). In addition, the first plurality of transformation units comprise a plurality of substitution units coupled to the first and the third register to receive the stored content of the first register, make at least partial substitution to the received content and store the at least partially substituted content into the third register during a round of operation (see Feistel, Figure 1, step 6; Figure 3A, So and S1).

12. As per claim 24, Feistel discloses a cipher system as outlined above in the claim 19 rejection under 35 U.S.C. 103(a). In addition, the first plurality of transformation units comprise a linear transformation unit coupling the second register to the first register to store a linearly transformed version of the content of the second register into the first register, taking into consideration inputs from the first key section, during a round of operation (see Feistel, Figure 1, step 3; Figure 3A).

13. As per claim 25, Feistel discloses a cipher system as outlined above in the claim 19 rejection under 35 U.S.C. 103(a). In addition, the first plurality of transformation units comprise a linear transformation unit coupling the third register to the second register to store a linearly transformed version of the content of the third register into the second register, taking into consideration inputs from the first key section, during a round of operation (see Feistel, col. 4, lines 7-26; Figure 1, step 6).

14. As per claim 26, Feistel discloses a cipher system as outlined above in the claim 19 rejection under 35 U.S.C. 103(a). In addition, the second key section comprises one or more linear feedback shift registers to output a first, a second and a third plurality of data bits; and a combiner function coupled to the LFSRs, and having a network of shuffle units serially coupled to each other, to combine the third plurality of data bits using the first and second plurality of data bits (see Feistel, Figure 1, 'Random Number Generator'; see Coulthart, Figure 1).

15. As per claim 27, Feistel discloses a cipher system as outlined above in the claim 19 rejection under 35 U.S.C. 103(a). In addition, the mapping section comprises a plurality of logical gates coupled to the third and sixth registers of the data and first key sections respectively to generate the pseudo random bit sequence (see Feistel, Figure 1, Reference Number 22; Figure 3A, 'Mangler').

16. As per claims 1, 2, 4-12, and 14-18, they are apparatus claims corresponding to claims 19, 21-27 and they do not teach or define above the information claimed in claims 19, 21-27. Therefore, claims 1, 2, 4-12, and 14-18 are rejected under Feistel in view of Coulthart for the same reasons set forth in the rejections of claims 19, 21-27.

17. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Feistel in view of Coulthart as applied to claim 19 above, and further in view of Schneier Applied Cryptography 2nd Edition (hereinafter Schneier). As per claim 20, Feistel discloses a cipher system as outlined above in the claim 19 rejection under 35 U.S.C. 103(a). Coulthart discloses a second plurality of transformation units coupled to the fourth and the sixth register to receive the stored content of the fourth register and store the transformed content into the sixth register during a round of operation. Coulthart does not disclose a substitution unit as a transformation unit coupled between the fourth and sixth register. However, substitution manipulations are often interpreted in very broad terms. Schneier teaches a running-key cipher which is a type of substitution cipher whereupon one text is used to encrypt another text (see Schneier, page 12, 1st

paragraph). In view of this interpretation of substitution, the XOR operators (E01, E02, E03), which combine the contents of the counter and the contents of the fourth register are substitution units that store the transformed content into the sixth register (see Coulthart, Figure 1). It would be obvious to one of ordinary skill at the time the invention was made to include a substitution unit as one of the transformation units coupled between the fourth and sixth registers since the transformation unit between the fourth and sixth registers as disclosed by Coulthart is inherently defined as a substitution unit as taught by Schneier.

18. As per claims 3 and 13, they are apparatus claims corresponding to claim 20 and they do not teach or define above the information claimed in claim 20. Therefore, claims 3 and 13 are rejected under Feistel in view of Coulthart as applied to claim 19 above and further in view of Schneier for the same reasons set forth in the rejection of claim 20.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Feistel U.S. Patent No. 4,316,055 discloses a stream/block cipher cryptographic system.

Hardy et al. U.S. Patent No. 5,195,136 discloses a method and apparatus for data encryption or decryption.

Chou U.S. Patent No. 6,167,136 discloses a method for preventing copying of digital video disks.

McDonough U.S. Patent No. 6,452,959 discloses a method and apparatus for generating data sequences for communications.

Matsui et al. U.S Patent No. 6,466,669 discloses a cipher processor and cipher processing method.

Faber et al. U.S Patent No. 6,477,252 discloses a digital video content transmission ciphering apparatus, which was copending with the current application.

Stallings Cryptography and Network Security 2nd Edition Chapter 3 discloses an overview of block ciphers.

Schneier Applied Cryptography 2nd Edition Chapters 12-17 discloses an overview of block ciphers, stream ciphers and RNGs.

Infocus 'Digital Visual Interface (DVI)' is a white paper on DVI.

Schneier et al. 'Unbalanced Feistel Networks and Block-Cipher Design' discloses an alternative to the classic balanced Feistel cipher.

Silicon Image 'High-bandwidth Digital Content Protection' is a white paper on HDCP.

Intel 'High-Bandwidth Digital Content Protection System' is an overview of HDCP.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00 A.M. to 5:00 P.M..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Jung W Kim
Examiner
Art Unit 2132

Jk
September 23, 2003

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100